Europe’s fragmented approach towards cyber security

Karine e Silva

On March 18, 2013, internet users worldwide felt the consequences of a massive cyber-attack. The biggest in history, the Distributed Denial-of-Service Attack (DDoS) of 300Gbps started as a retaliation from the hosting server Cyber Bunker against the anti-spam organisation Spamhaus. The attack not only caused disturbances to Spamhaus and its hosts and partners, but also slowed down internet connection internationally, most notably in the UK, Germany and other parts of Western Europe. In recent years, cyber security concerns have spread to different areas of life, with discussions over the impact of threats and need for resilience receiving growing media attention and significant government investments. This article examines the status of the cyber security debate in Europe, conflicts of interest in the private sector and perspectives from civil society.

The origin of Cyber security and the spread of cybercrime

Issues over the security of information and communication technologies (ICTs) have long accompanied cyberspace discussions (ITU, 2005). Despite undergoing significant changes on the agenda of various countries since the 1980s, the cyber security debate as part of national security policies (and as known today) started in the U.S. in the mid-1990s. From there, it started spreading to other technology dependent countries and their security programmes (ITU, 2005). The issue of network security was later complemented by concerns of attacks on critical infrastructure and their severe impact on national security and state economic welfare (Dunn & Wigert, 2004).

If cyber security is not a novelty, what has brought the issue to the centre of our current economic and political debate? For one thing, the development of ICTs has made nations’ welfare increasingly dependent on the services and advances of the information society, while leading to a major increase of the cyber threat spectrum (Dunn & Wigert, 2004). In Belgium, authorities reported an increase in computer crime offences and internet fraud of 75% between 2008 and 2010, while the German Federal Criminal Police Office (BKA) saw a 150% rise in cases of "phishing" in the same period. The growth and intensity of cyber-attacks has been reinforced by the availability of cheap, ever more sophisticated, rapidly proliferating and easy-to-use (and easy-to-find) tools that can result in powerful disruptions (Dunn & Wigert, 2004). Cybercrime has benefited from the complexity of technology, increase of internet penetration and lack of territoriality in cyberspace (Ghernaouti, 2013). Overall, these changes have resulted in large-scale attacks where the identity of criminals is protected or difficult to trace (Clough, 2011).

Though cyber security started as a matter of national security, today this is no longer the case. The issue has grown out of governments' agendas and companies’ risk management to become part of users’ daily life. Due to its potentially massive impact, the consequences of security breaches are not to be underestimated. Although government and business are most generally aware of the economic and social cost of cyber security, it has been particularly difficult to accurately estimate the danger and provide cost-efficient responses. Available statistics on the appropriate investments in cyber security and actual losses resulting from cybercrime are still insufficient, fragmented and often biased (Anderson & Al., 2012). Despite the differences in numbers, governments, researchers and the private sector are unanimous in estimating the social cost of cyber threats to be among the greatest menaces (Bauer & van Eeten, 2009).

The lack of a common understanding

Terminology has been a significant issue in the cyber security debate as a common understanding of cyber security is still lacking. Governments have attained to build safe online environments through so-called cyber security policies. While cyber security comprises several aspects of ICT security in the online and offline world,

internet safety is only part of the cyber security agenda. Often listed as a goal in countries' strategies, internet safety concerns a culture of awareness, responsibility and preparedness of individuals and organisations to cope with online threats.

Following the deliberations of the World Summit on the Information Society (WSIS) of 2005, the International Telecommunication Union (ITU), the United Nations agency responsible for ICTs, was given the mandate to coordinate international efforts in the field of cyber security. In 2010, the ITU Plenipotentiary Conference in Guadalajara, Mexico, strengthened this mandate through Resolution 130. Despite the content of Recommendation ITU-T X.1205, which encompassed an extensive concept of cyber security to be used internationally, states have spoken of cyber security without mutual understanding. Be it for the lack of states' interest in reinforcing international authority in the field of internet governance or for the inability of the United Nations in involving civil society by focusing mainly on reaching out to policy makers, the fact is that countries have established cyber security policies according to their individual needs. In this process, little consideration has been given to building an internationally reliable definition of cyber security. This is the reason why the understanding of the term varies from country to country (ENISA, 2012).

The need for a common understanding over cyber security has been called to attention by the European Union Agency for Network and Information Security (ENISA). Nevertheless, the recently launched Cybersecurity Strategy for the European Union failed to provide a clear definition of cyber security and to compel member states to introduce harmonised policies. Instead, it focused on establishing general principles of access, responsibility, fundamental rights and democratic governance, in addition to defining the role of governments in fighting cybercrime and strengthening national defence and international cooperation. The omission can be explained by members' lack of interest in trusting the EU with an area that allegedly belongs to their national security. While the borderless character of the internet requires a consistent approach across the Union, the overall EU cyber security status is fragmented. On the one hand, member states whose economy and infrastructure heavily depend on ICTs have taken action long before the introduction of the strategy. On the other hand, some members still struggle to implement basic steps towards cyber security, such as specific legislation and national response teams (CERTs). It is not surprising, thus, that heterogeneous cyber security policies and unequal levels of protection coexist inside the EU.

French Foreign Affairs have emphasised the vagueness of the word cyber security as a "blanket term" that encompasses the need for cyber defence and information system security alongside the fight against cybercrime. This terminology imprecision became evident in France's strategy for Information systems defence and security. The strategy also reveals France's choice for a government-ruled approach, where the state plays the main role in ensuring security. Britain has a similar vision, as the UK Cyber Security Strategy suggests that despite the importance of private sector and society, cyber security remains a national security topic and therefore part of the government agenda. Understanding the need for improved parameters and multistakeholder participation, The Netherlands established their own concept for cyber security and decided to tackle the issue with 'cooperation partners'. This collaborative system is embedded throughout the Dutch motto 'strength through cooperation'. This characteristic is also observed in Germany. The German strategy went far in presenting concepts of cyber security divided along civilian, national, global and military lines. However, here again cyber security is defined as an open and all-embracing idea. Such broad definition not only undermines the value and application of the term, but opens possibilities for 'cyber security' to be used for multiple and indiscriminate purposes.

Although all the above-mentioned strategies were issued in the first semester of 2011, little resemblance exists among the instruments. It seems that cyber security in the EU suffers not only from a lack of consensus in terminology, but also in how responsibility should be allocated among stakeholders, let alone weaved together in a coherent plan of action. While it is hard to say whether the inconsistent methodology has hampered a broader confrontation of the problem within the Union, the noticeable organisational and tactical divergences do reveal issues of coordination and information exchange. As the Cybersecurity Strategy for the EU brings new standards and guidelines, it is not yet clear whether member states will continue to act individually and primarily focus on their own needs. In the words of Dutch MEP Sophie in t' Veld (Alliance of Liberals and Democrats for Europe), "if you look more closely, you can see that this strategy is not a strategy, it's just a

mishmash of different measures and I think we are on a slippery slope.”

The private sector’s role

While private sector has sided with public authorities to fight cybercrime, but discussions over security strategies and business’s duties have divided opinions. Two distinguished groups can be identified here, often holding antagonists interests. The first, claiming more stringent control, includes computer security companies, risk management consultants, copyright holders, and the defence industry (Deibert, 2011). The second, mainly composed of internet service providers (ISPs), telecom operators, and the ICT equipment industry, defends minimum government intervention, free internet governance, and self-regulation. This said, cyber security has impacted business unevenly. While it is possible to argue that cyber threats are increasingly affecting the private sector, data from UNODC reveals that the proportion of European companies experiencing data corruption due to malicious software or unauthorised access is greater for large than for medium enterprises, which, in turn, is greater than for small enterprises. Although data corruption does not reflect the entire range of ICT vulnerabilities, it does reveal cybercriminals’ preference for larger business entities, possibly due to the value and sensitivity of the stored data.

Be it for their business interests or mission in protecting the world against cyberthreats, the computer security industry has demonstrated strong interest in being involved in the cyber security debate. In fact, companies like McAfee and Kaspersky have played an important role in shaping cyber security in the world. McAfee has designed special lines of products targeting government IT security aimed at protecting energy, healthcare, defence, federal, local and civil interests. The recent appointment of Phyllis Schneck, McAfee’s Chief Technology Officer (CTO), as the new head of the United States Homeland Security cyber security division demonstrates the high regards of the company before the government. Besides hosting Government Security Forums, where leaders of states, finance and technology are brought together to discuss integration of public policies and defensive technologies, Kaspersky sits at the International Advisory Board of IMPACT, ITU’s cyber security executing arm. The cooperation between the Russian anti-virus giant with police and intelligence agency authorities has raised allegations of ties with Moscow, which have been strongly refuted by Kaspersky. The knowledge held by security companies is undisputable and an efficient cyber security strategy must include the private sector’s expertise. However, governments and society must bear in mind companies’ inherent business interest and scrutinise their contributions accordingly.

The question is, however, whether computer security companies have contributed to advertising a danger that is greater than reality. Referring to the conflict of interest that affects the computer security industry, researchers have noted that much of the available data concerning the cost of cybercrime and investments in information security are collected by organisations such as antivirus software vendors, which often have a particular view of a specific agenda to match. Corroborating this idea, studies have concluded, “survey data on information security trends and concerns are used to justify increased expenditures on security tools and technologies. (…) The numbers, however, are anecdotal, are not generalizable to the business level, and are reported in cumulative form. In a word, they are not useful." Therefore is not surprising that computer security companies have claimed larger investments in cyber security and become government allies in implementing public policies for ICT securitisation.

Again, the ICT private sector is not a homogenous group. ISPs, mobile operators, and ICT equipment manufacturers have apparently stood on the opposite side of computer security companies. They argue internet regulation has gone far enough and that no additional legislation is needed. Internet giant Google has exercised enormous influence in lobbying against “burdensome” and “undemocratic” regulation. This was the case with SOPA and PIPA, as well as with the ITU World Conference on International Telecommunications (WCIT) in 2012. In both cases, Google successfully maneuvered users' support to block government negotiations and protect its business strategy. Stronger internet regulation could require Google to leave inertia and proactively stop cybercrime and intellectual property offences linked to its services, as well as to fully respect data protection in its operations and search results. Clearly, the internet services corporation has no interest in abiding to tougher laws, as monitoring user data and allowing free data traffic are some of the

reasons why the company remains market leader. Other companies have performed a less remarkable but still important influence. Cisco and Oracle have openly demonstrated their support to self-regulation and voluntary industry-led approaches to cyber security, while discouraging governments to play an active role in regulating the security industry.

Albeit significant parts of the ICT industry claim for voluntary cooperation as the way to go, self-regulation has fewer supporters outside. “Reliance on voluntary action and proselytizing the adoption of best practices guarantees inadequate security,” sustain researchers from Washington D.C. (Lewis, 2005). The failure of market regulation for implementing cyber security standards has been acknowledged by ENISA in the Flash Note FN/02/2013, when examining that cases like the Spamhaus DDoS attack could be avoided if network providers would implement recommendations that have been around for almost 13 years. Although the impact of security breaches amount to sufficient incentives for companies to adopt high security standards, business shortfall in cyber security investments are a true market failure and the reason why some have called for government intervention in the field (Lewis, 2005).

Finally, internet securitisation has also been attained by government pressure over the private sector. ISPs are now increasingly active as the new internet police (Deibert, 2011). As noted by Susan Infantino, Google’s Legal Director, “it’s become increasingly clear that the scope of government attempts to censor content on Google services has grown.” Her statement can be illustrated by the numerous requests made by the governments of reportedly democratic states aimed to take down content from Google’s website and related services (Deibert, 2011). Whereas the removal of specific malicious data can be necessary to safeguard fundamental rights, examples of politically motivated requests are not infrequent. Recent cases of politically driven requests have involved Italy, Hungary, France and Spain. “We’ve been asked to take down political speech. It’s alarming not only because free expression is at risk, but because some of these requests come from countries you might not suspect — Western democracies not typically associated with censorship," criticises Google.

Civil society’s perspectives

Making users aware of the risks of ICTs and capable of deploying basic mechanisms of protection can contribute to promote a safe, trustable and inclusive information society (Ghernaouti, 2013). While awareness raising and capacity building have long been addressed as important elements of any cyber security strategy, the prevalence of aspects such as national defence have overridden the interest for a user-driven internet safety approach and even threatened long-standing fundamental rights.

Reality reveals increasing concerns over the use of cyber security for introducing and legitimising means of government surveillance and restrictions to freedom of speech (Comninos, 2013). For activists, the use of cyber security policies has justified greater territorialisation of cyberspace controls (Deibert, 2011). Researchers from the universities of Cambridge and Harvard indicate internet censorship tools created for a legitimate reason can be later deployed for a different purpose, and say the practice is not restricted to authoritarian countries (Murdoch & Roberts, 2013). Recent attempts of censorship through law include cases in democratic nations, such as the UK, with a system for blocking images of child sexual abuse being used to block The Pirate Bay Bit Torrent search engine (Murdoch & Roberts, 2013). The polemic Access Impediment Law (*Zugangserschwerungsgesetz*) in Germany, and the discussions surrounding the Stop Online Piracy Act (SOPA), the Protect IP Act (PIPA) (Bambauer, 2012), and the Cyber Intelligence Sharing and Protection Act (CISPA) in the United States are just a few more examples. Finally, the civilian surveillance scandals of 2013 showed how Western democracies have used the law to justify restrictions to citizens' right to privacy. In response to the leakage of the National Security Agency international monitoring scheme, the U.S. Justice Department released a legal memorandum explaining why the government believes it is lawful under a provision of the Patriot Act known as Section 215 for the N.S.A. to collect and store logs of every phone call dialed or received in the country.

Although the speech for cyber security can be misused for censorship and social control (and it has been), cyber security should not be interpreted as a tool aimed to restrict citizens’ fundamental rights. In the

occasion of the Tunis Agenda, states were called upon to affirm "that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression." In fact, states will not be able to protect and promote human rights online without adequate cyber security. With regards to content restriction, many countries consider material such as child pornography, racism, and hate speech sufficiently objectionable to want to prevent their dissemination (Bambauer, 2012). Measures deployed to prevent the availability of malicious content, however, cannot be used to impair freedom of speech.

A civil society approach requires a shift in how cyber security is seen, moving from the national security sphere to become part of the public interest. Strategies and policies to secure internet should focus in realising society's wishes in keeping cyberspace open, free and prone to innovation. "As a society the culture of the Internet is much more about open-ness and experimentation than about safety and security," says academic Steven Weber in the Harvard Business Review. In fact, activists have considered the term security as anathema of a global civil society (Deibert, 2011) and demonstrated their lack of faith in the progressive securitisation of cyberspace (Comninos, 2013). They urge policy-makers to prioritise the security of individual users, civil society and organisations' networks, over excessive regulation and militarisation of the Internet (Comninos, 2013). This debate certainly calls for greater civil society participation and empowerment in the political decision-making, as the cyber security issue has been strategically kept away from society's influence.

Conclusions

Without a clear definition, cyber security will continue to be used for multiple and occasionally contradictory purposes. The broad application of the term has led to fragmented approaches within the EU and justified recent restrictions to privacy and freedom of speech in democratic nations. While states fight to keep the issue under national authority, reality has showed that despite the public good characteristic of cyber security, individual stakeholders make most information security decisions (Bauer & van Eeten, 2009). This decentralisation has led to sub-optimal security levels (Bauer & van Eeten, 2009), as it answers to the private interests of specific actors and has little regard for public interest. A user-driven approach to cyber security would guarantee that individuals are prepared to deal with cyber threats and protected from interferences in the exercise of their rights online. Discussions around the EU's Cybersecurity Strategy and the final works in the revised OECD Guidelines for the Security of Information Systems and Networks reveal, however, that we are still to wait for a harmonised concept of cyber security. Even longer, one can think, for a society-centred perspective.

References

Anderson, R. et al. (2012). Measuring the Cost of Cybercrime. WEIS. Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Bambauer, D. E. (2012). Censorship V3.1. 18 IEEE Internet Computing 26 (May/June 2013). Arizona Legal Studies Discussion Paper No. 12-28. doi:http://dx.doi.org/10.2139/ssrn.2144004

Bauer, J.M., & van Eeten, M.J.G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy, 33(10–11), 706-719.

Clough, J. (2011). Cybercrime. Commonwealth Law Bulletin, 37(4), 671-680.

Comninos, A. (2013). A cyber security Agenda for civil society: what is at stake? APC Issue Papers. Retrieved from http://www.apc.org/en/system/files/PRINT_ISSUE_Cyberseguridad_EN.pdf

Deibert, R. (2011). Towards a cyber security strategy for global civil society? Global Information Society Watch. Retrieved from http://www.giswatch.org/sites/default/files/gisw_-_towards_a_cyber_security_strategy.pdf

Dunn, M., & Wigert, I. (2004). International CIIP Handbook 2004. Center for Security Studies, ETH Zurich. Retrieved from http://mercury.ethz.ch/serviceengine/Files/ISN/452/ipublicationdocument_singledocument/72b87f2b-61bd-4122-acbf-4c689532036a/en/doc_454_290_en.pdf

European Network for Information and Security Agency. (2012). National Cyber security Strategies: Practical Guide on Development and Execution. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Ghernaouti, S. (2013). Cyberpower: crime, conflict and security in cyberspace. EPFL.

International Telecommunication Union. (2005). A comparative analysis of cybersecurity initiatives worldwide. Retrieved from http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Lewis, J.A. (2005). Aux armes, citoyens: Cyber security and regulation in the United States. Telecommunications Policy 29, 821-830.

Murdoch, S.J., & Roberts, H. (2013). Internet Censorship and Control. Retrieved from http://ssrn.com/abstract=2268587